

The 2024 Duo
Trusted Access Report

CISCO



**Navigating
Complexity**



The 2024 Duo Trusted Access Report



Table of contents

The New Frontier of Access Management and Identity Security	3
Methodology	5
Key Findings	5
01 Billions of Authentications	7
Stronger Auth Methods Show Upward Trends	8
Return-to-office is the New Hybrid Work Reality	10
Futureproofing Against Attackers	12
02 Attack Surface Increase	14
The Continuing Rise in Global MFA Usage	14
Identity is the New Perimeter	17
The Talos Perspective	18
03 Establishing Device Trust	19
A Diverse Device Environment	19
Device Visibility: Protecting What You Can't See	23
Authentication with Out-of-Date Software	24
04 Powerful Policy Controls	27
Learning From When Authentications Fail	27
Benefits of Strong Device-Based Policies	29
Top 3 Policy Groups to Reduce Security Debt	30
+ Closing Words	34
The Future of Identity Security	34
Context is the New MFA	35
Recommendations	36

Trusted Access Report Legend

- | | |
|-------------------|------------------------|
| Start of section | Point of interest |
| Section continues | Additional Information |
| End of section | |



MFA is a great security measure, but not enough on its own. More sophisticated threats call for additional layers of security.

Introduction

The New Frontier of Access Management and Identity Security

In exploring the future, we're often drawn to predicting the unknown. Our quest for answers is unending, and we rely heavily on data to guide our predictions.

Organizations today navigate a treacherous digital landscape where the motives of attackers are as varied as their methods – ranging from financial gains, cyber espionage, and disruption to reputation damage to cyber warfare. Concurrently, these organizations also manage various internal complexities, from the intricacies of their IT stacks to dispersed hybrid workforces and a great variety of devices accessing their systems and applications. This evolution from ad hoc remote work setups to hybrid work models has extended the traditional enterprise perimeter to the far corners of the cyber realm.

Years ago, protecting an IT infrastructure might have been largely about ensuring that systems were running smoothly – the proverbial “keeping the lights on.” Now, the remit has expanded exponentially; it encompasses a vigilant defense against a host of external cyber threats, from ransomware to state-sponsored hacking. As the threat landscape has widened, so has the surface area for attacks, with every employee's access or device becoming a potential entry point. This shift has transformed IT departments from units concerned primarily with operational uptime to essential guardians against a spectrum of sophisticated external threats.

While we can't tell precisely what the future will bring, analyzing historical patterns provides insights into future possibilities. For instance, the previous edition of the Trusted Access Report pointed out the soaring adoption of multi-factor authentication (MFA) as companies have been looking to reduce risk in a more advanced security landscape.

As organizations grapple with increasingly sophisticated cybersecurity threats, a demand for holistic access management solutions has been apparent for a few years. MFA is a great security measure, but not enough on its own. More sophisticated threats call for additional layers of security.

By integrating context, an access management solution can analyze the situation in which access is being requested, such as information about the user's typical behavior or environment including their usual login times, geolocation and device. This adds an additional layer of security, providing a more holistic and dynamic approach to authentication.

In essence, adding context to the authentication process allows systems to better differentiate between legitimate users and potential threats, enhancing security while maintaining a good user experience. Thus, context becomes the new form of MFA.



Contextual factors such as location or device details (operating systems, for example) have been included in Trusted Access Reports for years. However, with hybrid work as a firmly ingrained reality, the importance of contextual factors carries even more weight.

Another area where we have detected a rising level of interest is the future of identity; more specifically ways of addressing proliferation of digital identities from the cybersecurity perspective.

In the modern workplace, every employee may have multiple digital identities across various systems, applications, and platforms. This can range from email accounts, to access credentials for internal systems, to profiles on collaboration platforms like Slack. As businesses continue to adopt cloud services, software-as-a-service platforms, and remote collaboration tools, the number of these digital identities grows. This proliferation has significant implications for both productivity and security.

On one hand, these identities can enable more seamless collaboration and access to necessary resources, improving efficiency. On the other hand, managing these numerous identities and ensuring they are properly secured becomes a complex task. Risk visibility across an organization's identity ecosystem in a single, comprehensive interface has become a must.

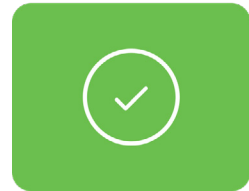
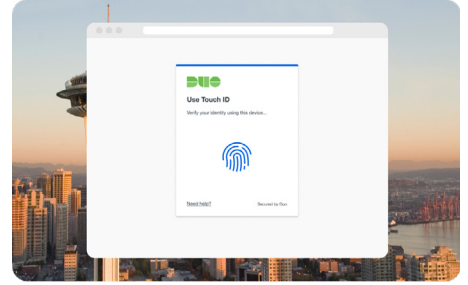
This can be achieved via identity threat detection and response (ITDR) capabilities. The evolution of ITDR is integral to the future of identity, ensuring that our digital identities remain secure as they become increasingly prevalent in our day-to-day lives.

The challenge is clear: as the MFA usage continues to expand globally, so do attackers' methods. To minimize chances of a breach, traditional MFA does not only need to be enhanced with contextual factors such as the user's typical behavior or environment but also the visibility across an organization's identity ecosystem in a single, comprehensive interface.



Methodology

In this report, we'll delve into insights drawn from an analysis of over 16 billion authentications in the last year (and over 44B in the last 4 years), spanning nearly 52 million different browsers, on 58 million endpoints and 21 million unique phones across regions including North America, Latin America, Europe, the Middle East, and the Asia Pacific. We defined our 2023 annual time range as between June 1, 2022, and May 31, 2023.



Key Findings

01

Stronger Auth Methods Show Upward Trends

Authenticator apps like Duo mobile appeal to both demand for higher security and ease-of-use, with 91.5% of accounts enabling Duo Push as a factor accounting for 21% or over 3.2 billion authentications. We also observed a decreasing trend in SMS and phone calls as a factor, dipping to an all-time-low with 4.9% of authentications—a 22% decrease from 2022.

02

Return-to-Office is the New Hybrid Work Reality

Last year, access to remote access applications fell to nearly 25% of authentications after peaking in 2020. The quantity of authentications in this category has continued to decline since then as more companies move staff back into the office.

03

MFA Usage Continues to Expand Globally

The number of MFA authentications using Duo rose by 41% in the past year, with countries like Germany seeing a 52.3% increase in authentications year over year. In the Asia-Pacific region, Japan, the Philippines, and Australia saw continued growth from last year, increasing by 28%, 24.9%, and 16.9% respectively. Brazil makes the third-highest increase in authentications seeing 26.3% more MFA usage from 2022.

04

Diverse Device Environments Require Vendor-Agnostic Security

While Windows continues to lead the pack comprising 38.2% of access devices, we note that iOS is a strong second at 33.4% in the overall operating system ranking. Apple continues to rule the roost in the mobile category amongst Duo users, with the nearest contender being Android, which has a far lower adoption rate at 28.2%. Eliminating potential security gaps, vendor-agnostic security also allows for greater flexibility and scalability as the security system can easily adapt to changes in the device environment.





Key Findings

05

Organizations are putting in stricter controls reducing risk of out-of-date software

The percentage of failures due to out-of-date devices increased by 74.7% in 2023.

The more operating systems (OS) an organization allows to authenticate, the more likely it is those authentications will occur with an out-of-date OS. Organizations – particularly those which are expanding their IT environments – are increasingly putting in stricter controls, aiming to reduce risks posed by out-of-date software.

06

Failed Authentications Highlight User Risks

5% of all measured authentications were ones that failed. When we further examined the data, we discovered that 28% of the failed authentications were due to the users not being enrolled in the system. Unenrolled users may gain unauthorized access to sensitive data or critical systems, leading to data breaches.

07

Top 3 Policy Groups to Reduce Security Debt

One of the most effective strategies for mitigating security debt is through the comprehensive management of risk. Policies addressing geo-restrictions, unsecure devices, and granular per-user or per-application access can help reduce complexity and increase security coverage. However, 96.4% of organizations have no policy related to location (allow, deny, or require 2FA).

08

Identity is The New Perimeter

Without proper visibility, threat detection, and response, identity infrastructure provides ample opportunity for attackers to enter critical systems. In 23% of engagements observed by Talos IR, attackers were able to abuse compromised credentials to access valid accounts¹. The average company has 40.26% of accounts with either no MFA or a weak MFA².



In an environment where sophisticated cyberattacks have become the norm, an access management solution needs to be enhanced with identity threat detection and response capabilities, offering visibility across an organization's identity ecosystem in a single, comprehensive interface.



Footnotes:

1. From [Talos IR 2023 Year In Review](#), see "Telemetry Trends" pg. 6-7

2. From the [State of Identity Security](#) report (Oort), see Section 2 "Multi Factor Authentication: Full Coverage Remains Elusive"

01

Billions of Authentications



MFA continues to strengthen passwords

Multi-factor authentication holds strong while adding to the security of traditional password usage. The number of MFA authentications using Duo rose by 41% in the past year.

Push preferred

Duo Push is the most-used authentication method, accounting for 21% of all authentications.

Passwordless adoption continues to rise

Account adoption of WebAuthn-enabled factors, including security keys and biometric technology like TouchID, increased by 53% from 2022 to 2023 alone.

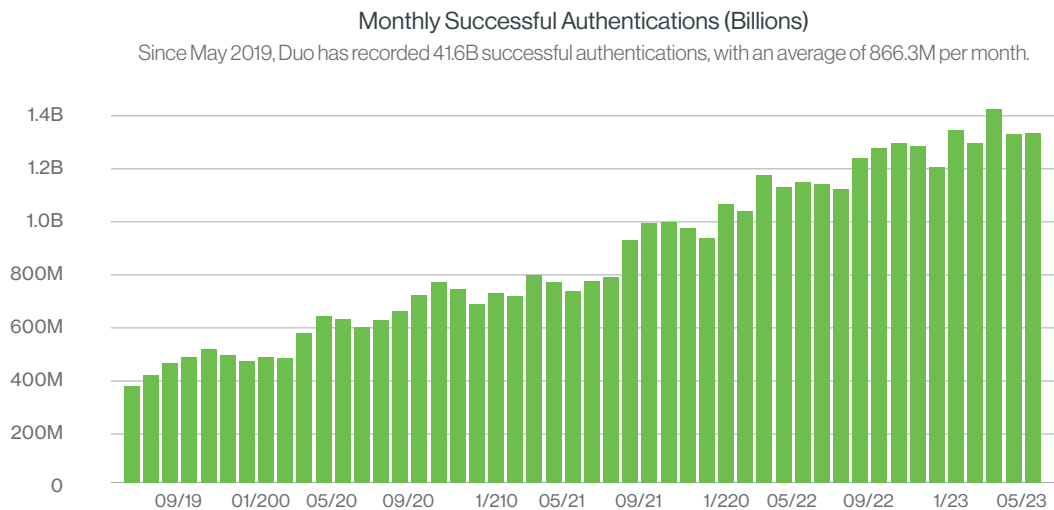


Figure 01 Monthly successful authentications





Stronger Auth Methods Show Upward Trends

The weaknesses of passwords as a sole authentication method are well-documented. They can be guessed, cracked, phished, or stolen, and users often exacerbate these vulnerabilities by reusing passwords across multiple services or creating simple, easily decipherable passwords. In contrast, multi-factor authentication (MFA) mitigates these risks by introducing additional hurdles for potential attackers. Even if a password is compromised, the chances of an attacker also having access to the user's physical device or biometric information are significantly lower.

However, recent high-profile cyber-attacks have shown that simply enabling a second factor does not make an account impenetrable. Not all authenticators are born equal, with factors like FIDO2 security keys and WebAuthn-enabled biometrics proving harder to exploit compared to weaker, but more accessible, factors like SMS text or phone call.

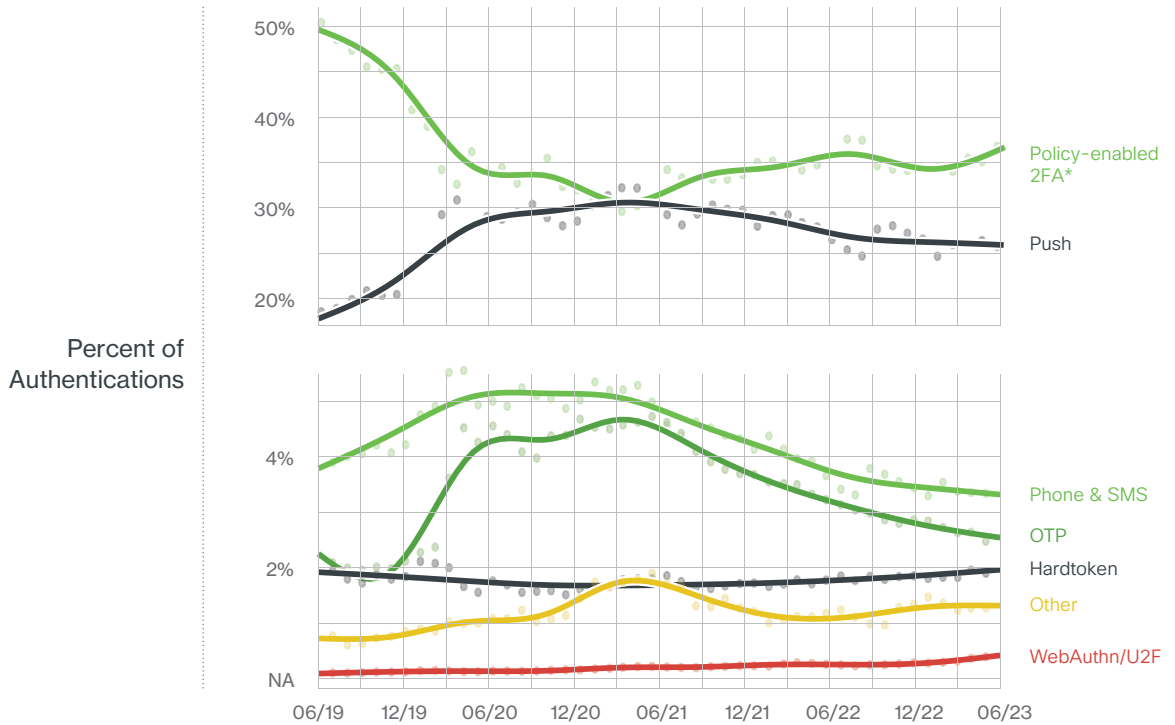


Figure 02 Authentication percentage over time by factor count

*In this context, Policy-enabled 2FA includes authentications where the user was assigned **bypass status** or enabled Duo Remembered Devices on their account, providing strong authentication for users while maintaining a seamless, non-disruptive login experience. Duo **Risk-Based Remembered Devices** adds additional security to Duo's Remembered Devices feature by adapting the duration of remembered device sessions in response to risk signals.



Percent of accounts using WebAuthn

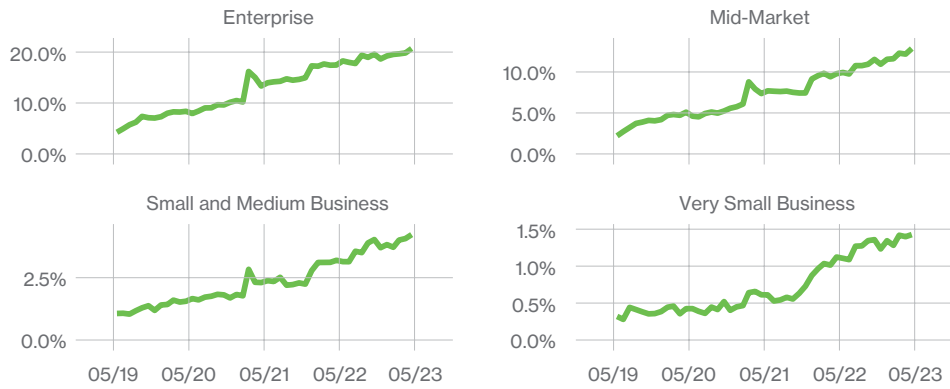


Figure 03 Percent of accounts using WebAuthn for authentication

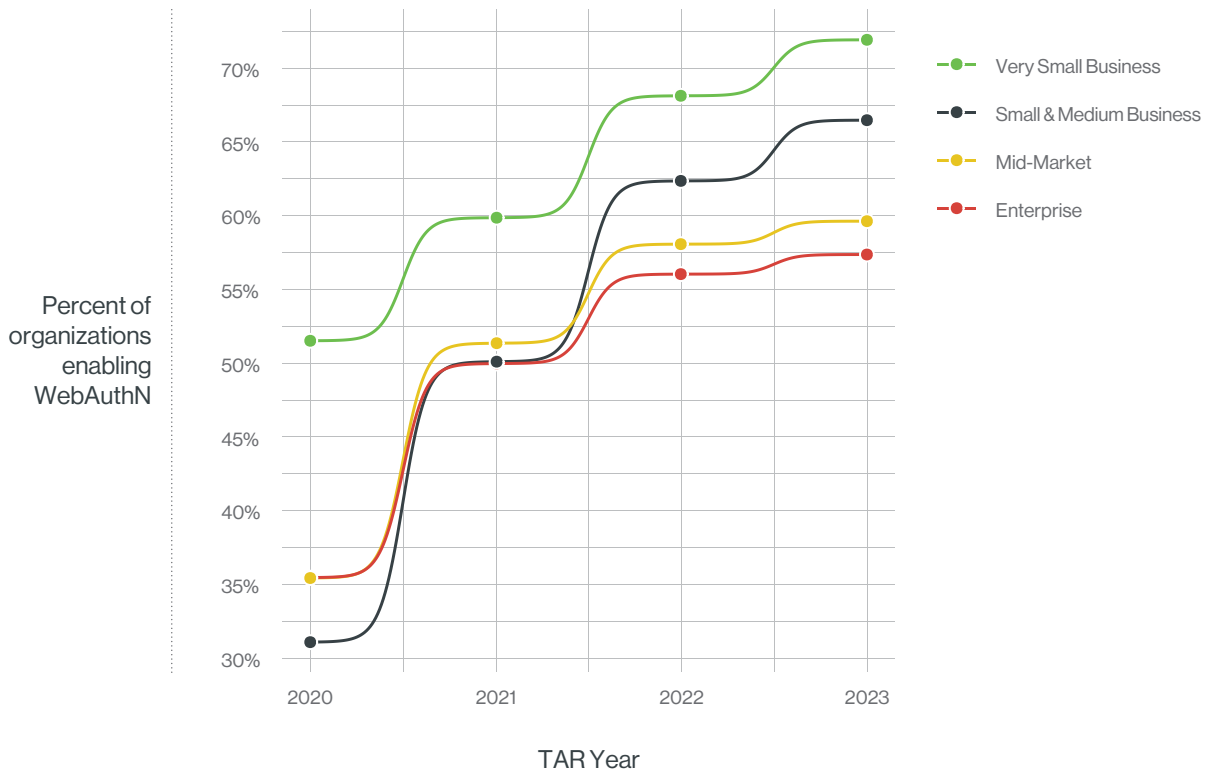


Figure 04 WebAuthn adoption by market segment

Luckily, authenticator apps like **Duo Mobile** appeal to both demand for higher security and ease-of-use. 91.5% of accounts enable Duo Push, a one-tap authentication available via the Duo Mobile application, accounting for 21% or over 3.2 billion authentications. We also observed a decreasing trend in SMS texts and phone calls as a factor, dipping to an all-time-low with 4.9% of authentications – a 22% decrease from 2022. More secure methods like WebAuthn and hard tokens take their place as the benefits of phishing-resistant MFA and smarter access policies gain traction amongst SMB and enterprises alike.



Return-to-Office is the New Hybrid Work Reality

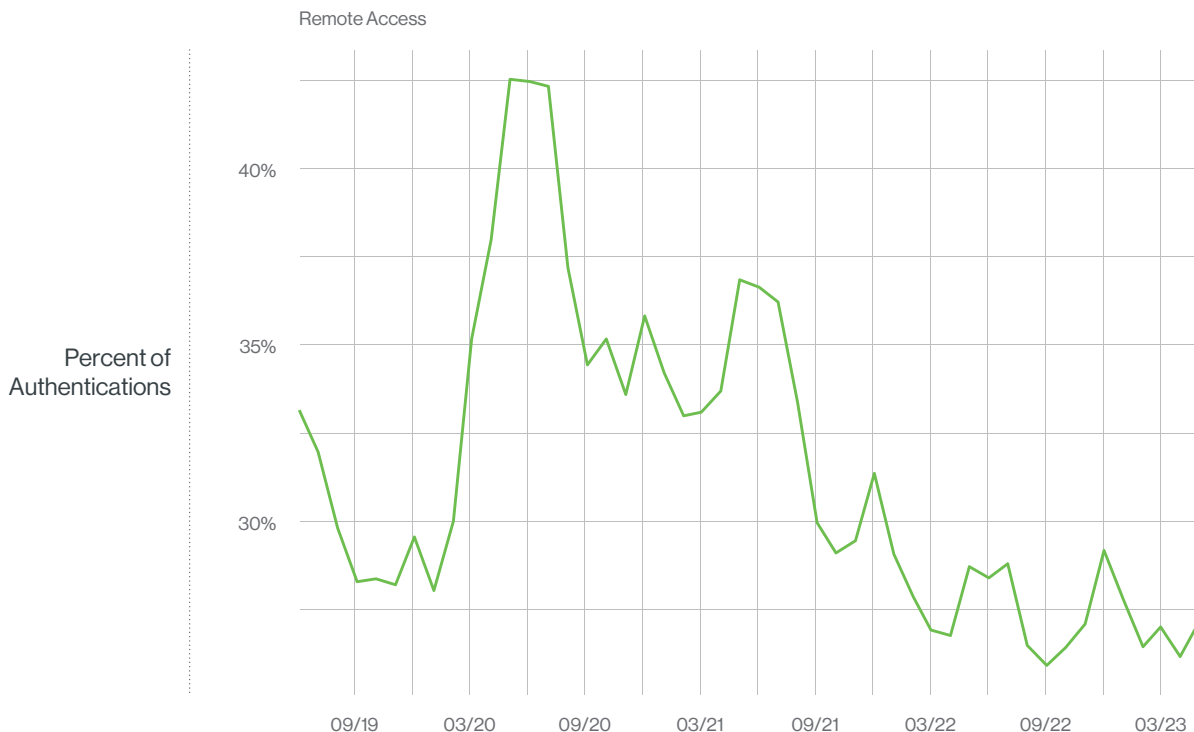
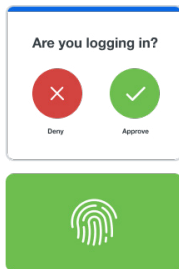


Figure 05 Authentications for Remote Access Applications

Remote access applications are software apps that allow a user to remotely access and control another computer or network over the internet or a local network connection. These apps are used for various purposes including troubleshooting, file transfers, remote administration, or accessing files and software on an office computer from a remote location.



Last year, the number of authentications for remote access applications reached nearly 25%. This is lower than pre-pandemic levels after the peak we saw in 2020. The quantity of authentications in this category has continued to decline since then as more companies move staff back into the office. While we observe a lower volume of authentications across the board during the December and January holiday periods, several industries including education, retail, and healthcare spiked during the first calendar quarter.



Let's set the scene...

With the return of business travel, designated in-office policy, or even just flu season, predictable ebb and flow of authentication requests begin to fluctuate. The cadence breaks as employees take leave, work remotely, or operate on varied schedules. These changes can lead to a surge in remote access requests, with employees reaching out to corporate networks from a multitude of locations and devices, not just their usual work terminals. Consequently, the IT systems must handle an influx of mixed on-premises and off-site login attempts with a greater reliance on VPNs and other remote access technologies.

Moreover, seasonality can also bring about an increase in temporary staff as businesses scale up to meet demand. This influx requires the creation and management of additional temporary credentials, a wave of new entries into the authentication system. Once the season wanes, there's a corresponding outflow as these seasonal credentials are revoked.

This variance does not merely alter the volume, but also the nature of authentications. There is a heightened need for robust security measures as the risk of cyber threats often spikes during these times. Thus, a layered security approach becomes even more crucial – with MFA as a minimum requirement.

During these peak times, the IT environment's authentication protocols must be both elastic and secure, expanding to accommodate the increased and varied load while maintaining the integrity of the system. IT staff remain on high alert to watch for any anomalous activity that could signify a breach attempt.



Futureproofing Against Attackers

The identity threat landscape is rapidly evolving, and trusted identity providers have fallen under attack. According to CISA, attackers are actively exploiting identity policy gaps to gain access to critical applications. Regardless of the increased risk, 85% of organizations feel they are not prepared and ready to protect themselves against modern attacks according to the Cisco Secure Readiness Index study³.

Visibility across the identity infrastructure is a must-have when addressing the types of attacks adversaries concoct. While there's been a significant uptick amongst MFA authentications through Duo, another piece of research suggests that security gaps are still across the market: the average company has 40% of accounts with either no MFA or weak MFA⁴. Especially in periods of change, strong access management and identity visibility is critical. For brief moments you might strike the right balance, only to be disrupted by new and emerging threats, changing user behavior, and a complex IT environment.

This is why modern security initiatives require continuous monitoring across identity, critical applications, and human resources information system (HRIS) versus a “set it and forget it” approach. As the security landscape evolves, many businesses are adopting a zero trust access policy strategy to mitigate modern attack surfaces. Organizations with a mature zero trust implementation score 30% higher in security resiliency than organizations without a zero trust strategy⁵.

In 2023, we saw a proliferation of two specific types of MFA-targeting attacks taking advantage of push-based authentications and unassuming users:

01



Push harassment

Multiple successive push notifications to bother a user into accepting a push for a fraudulent login attempt.

02



Push fatigue

Constant MFA means users pay less attention to the details of their login, causing a user to mindlessly accept a push login request.

Duo already supports WebAuthn FIDO2 authenticators, which offer the strongest protection against MFA-based attacks. However, we know that rolling passwordless out across an organization is a journey. It's encouraging to see that Duo Verified Push, a more flexible step-up factor that became generally available to all Duo customers during the data period of this report, was enabled on over 5,600 accounts.



As attackers' techniques become more sophisticated, a multi-layered defense system is crucial.



Trust in users is essential, but no longer enough. The addition of outside vendors and contractors adds complexity to closed, managed endpoint-only access policy. **Duo Trusted Endpoints**, made available to all Duo editions, adds an extra layer of security even if an organization cannot manage the device directly. Administrators can define a trust policy for every endpoint—whether managed or unmanaged, company-issued, contractor-owned, or personal—and stop attacker's unknown devices even if they are able to bypass MFA.



Increased friction often appears as a challenge to user adoption. As part of balancing security with productivity, we enhanced **Duo Remembered Devices** to account for changes in risk: when we recognize the device a user is on, we use a securely generated device token to authenticate so long as trust is maintained.



While access security should be tailored to the level of risk, organizations can struggle to get buy-in to add friction for every login. Duo's **Risk-Based Authentication** solution addresses this challenge—only stepping up to the more secure method when environment risk signals indicate there are potential threats, like location anomalies or known attack patterns. Whether security teams enable **Verified Duo Push** for all users, or through a risk-based approach, this allows organizations to make access security decisions based on their risk appetite and organization's needs.



IT teams must ensure that their Identity Security program is built on a strong foundation with the right tools, like strong MFA factors and intelligent step-up. Once these tools and policies are in place, **Identity Threat Detection and Response (ITDR)** can bolster an organization's identity security posture by arming the IT security professionals with both proactive and reactive tools.

ITDR helps proactively detect policy misconfigurations, identity-provider-to-HRIS discrepancies, and excessive privileges. It can also catch high-risk scenarios such as dormant or inactive accounts and accounts with MFA disabled—a trend noted in the 2023 Cisco Talos 'Year in Review' Report⁶. On the reactive side, the tool equips IT teams to respond to suspicious activities such as new MFA device registration, risky SSO sessions, superman (unrealistic travel) logins, access from a new device or location and more.




Footnotes:

3. See "[Cisco Cybersecurity Readiness Index](#)," which categorizes companies into four stages of readiness: from Beginner, to Formative, Progressive, and finally Mature, based on their preparedness across five keypillars and the state of deployment of 19 security solutions within those
4. From the [State of Identity Security report](#) (Oort), see Section 2 "Multi Factor Authentication: Full Coverage Remains Elusive"
5. Read more findings from the [Security Outcomes Report, Vol 3](#) published by Cisco (Renner)
6. Read all [Cisco Talos Year in Review](#)

Attack Surface Increase

The Continuing Rise in Global MFA Usage

Data shows that the global customer base protected by Duo’s multi-factor authentication security is continuing to grow. The number of MFA authentications using Duo rose by 41% in the past year, with countries like Germany seeing a 52.3% increase in authentications year over year. In the Asia-Pacific region, Japan, the Philippines, and Australia saw continued growth from last year, increasing by 28%, 24.9%, and 16.9% respectively. For the first year measured, Brazil makes the third highest increase in authentications seeing 26.3% more MFA usage from 2022.



41%

Rise of MFA authentication using Duo in the past year

This indicates a rising trend in the recognition of the importance of enhanced security measures predominantly as a response to a rising volume of cyber threats, but also as a reflection of international compliance requirements such as GDPR, C5, AgID, or HIPAA.

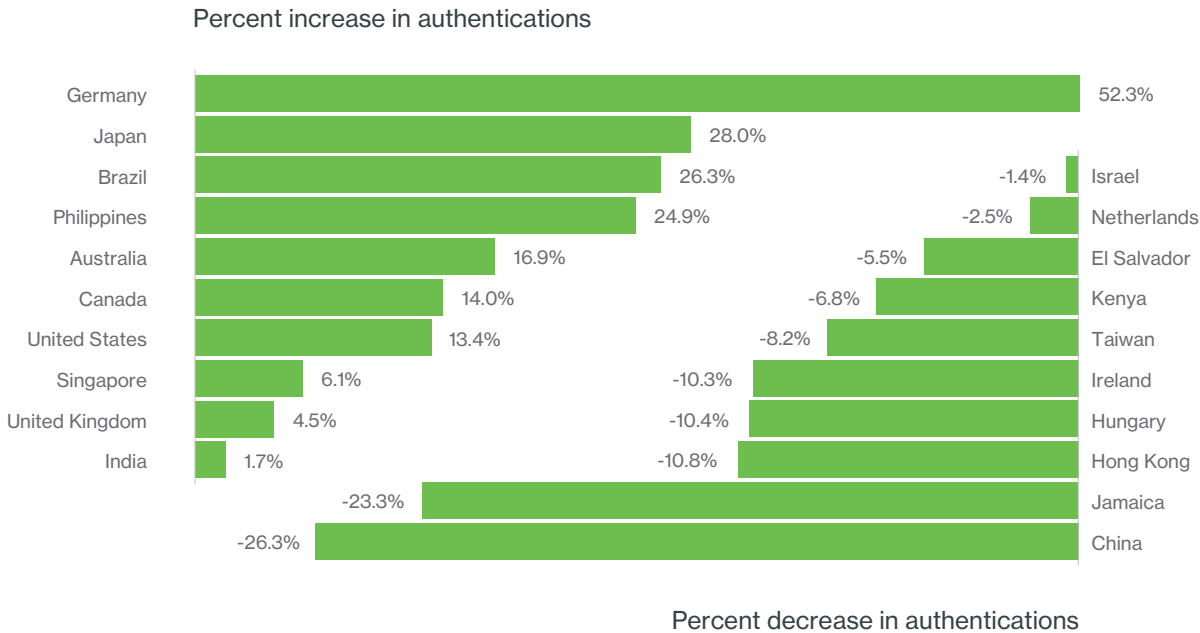
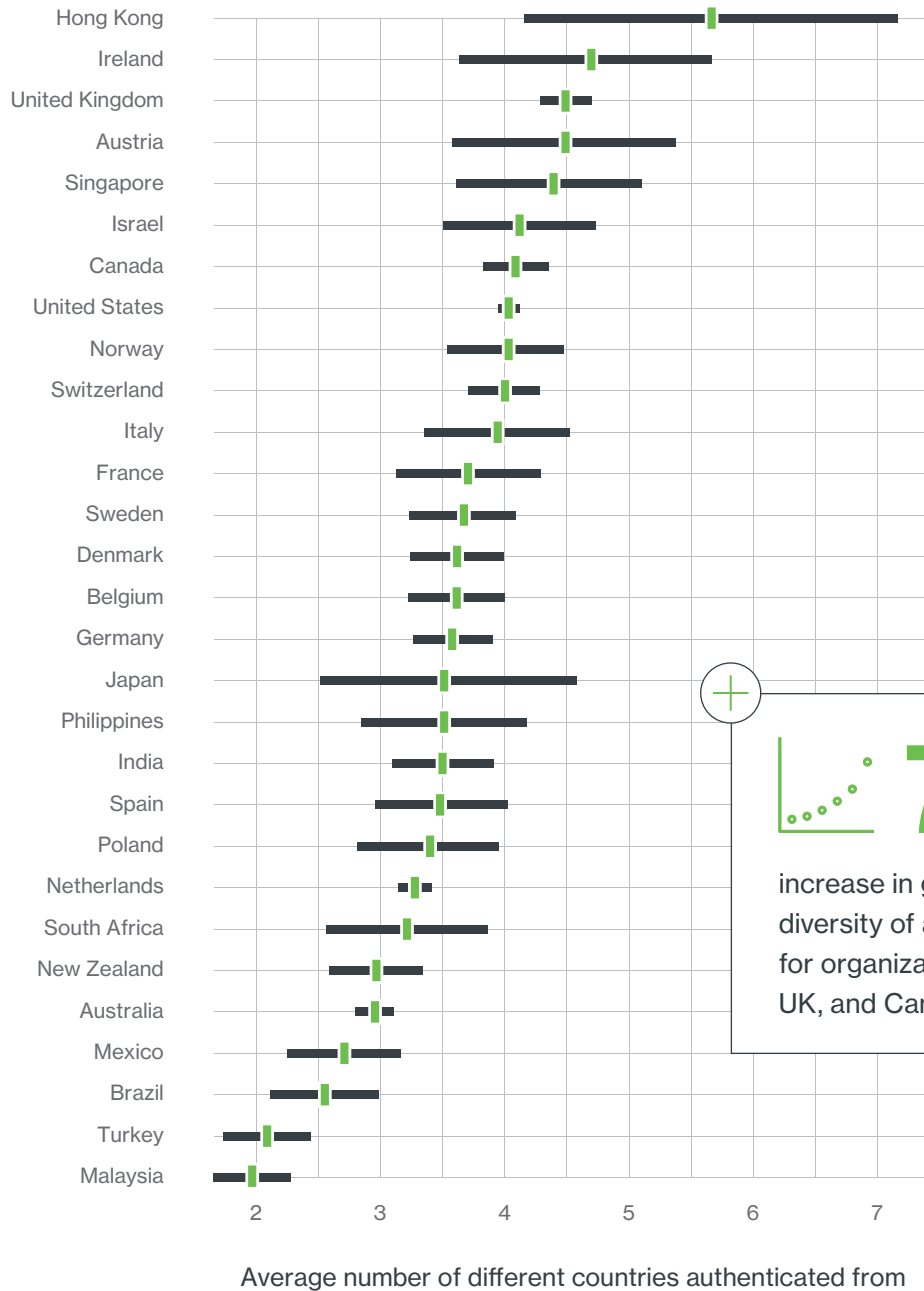


Figure 06 The top 10 countries that experienced an increase or decrease by authentication volume based on access device IP address

Organization
Country



72%
increase in geographic diversity of authentications for organizations in the US, UK, and Canada

Figure 7 Average number of different countries accessed by organizations of a particular country

In figure 7 we revisit a statistic we looked at last year, which is the geographic diversity from which an organization operates. In particular, we look at the average number of countries that we see users authenticate from when an organization is found in, say, Hong Kong. With continued diversification and spread of business interests, Hong Kong saw the highest average spread of authentication across 5.6 different countries on average. Organizations in the United States, Canada, and the United Kingdom saw authentications come in from an average of 4 different countries – a 72% jump from the 1.5 to 1.75 different countries on average seen last year.



An internationally dispersed workforce means more employees, contractors, clients, and third parties can access the organization's business's digital infrastructure from various locations, often on different devices, networks, and operating systems which can introduce additional vulnerabilities. Data and resources can be accessed from a greater scale of networks and endpoints. This helps support the concept that 'identity is the new perimeter' and 'context is the new MFA.' Identity security is a forever evolving problem and it's a daunting task for organizations to plug every hole the user journey creates.

In addition, an international presence does not only increase the variety in technology stack, but it can also add a wider array to the physical challenges of a more geographically diverse user base. Also, IT systems must cater to mixed tech stacks and varying data protection and privacy laws. This pushes the complexity that IT teams need to deal with yet another notch.

Globalization, like the organization size, increases the probability of a presence of more than one identity provider. Moreover, large organizations may acquire other companies, each of which may have its own existing identity provider. Instead of consolidating everything under one identity provider, which can be complex and disruptive, organizations sometimes choose to maintain multiple identity providers.

Managing identities increases in complexity with greater probabilities of supporting more than one identity provider (IdP). Without proper security measures in place, this can lead to potential security gaps or vulnerabilities that can be exploited for identity-based attacks like compromised credentials.



Global business practice requires broader, vendor-agnostic access management that helps organizations detect, respond to, and report attacks.

Identity is The New Perimeter

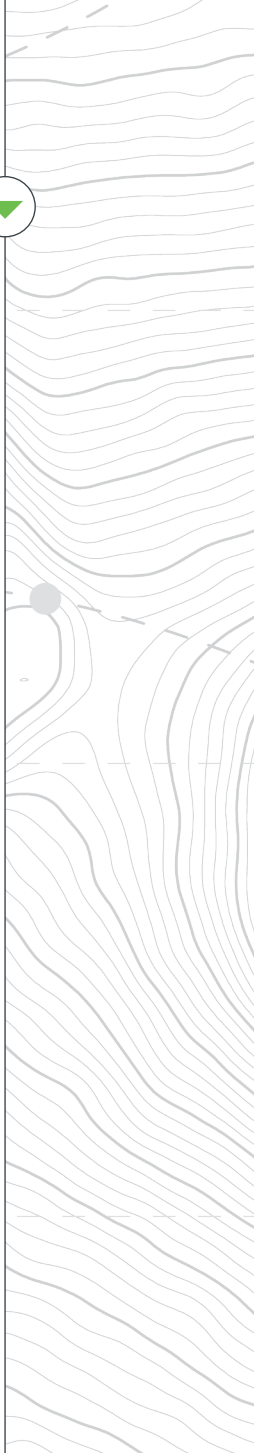
Identity security is a key part of access management. Securing and verifying identities allows an identity and access management (IAM) system to manage access to resources effectively and securely. Because of this, it's important to spend a few moments highlighting identity-security trends that have come to light when we were pulling together this report.

There are a few reasons why gaps in identity security occur. For some companies, the prompt comes from cloud migration. As companies grow and move their operations to the cloud, they often need to introduce new IAM systems but do not completely deprecate older IAM systems. For other companies it is migration from an on-premises directory to a cloud-based directory but keeping both. And the third group is composed of companies that have acquired one or more companies and support numerous identity platforms.

Another contributing factor comes in the form of operational challenges. Identity security often falls under the IT function and may not receive the attention and resources it needs to be effective. It requires investment in technology and personnel to manage and continuously monitor the IAM systems, ensure compliance with regulations, and respond to security incidents.

For some, cloud migrations and organizational scaling require the introduction of new IAM systems. Mergers and acquisitions, operational globalization, and a geographically diverse user base add even more complexity to keeping track of authenticating identities.

In the face of digital transformation, identity security may suffer from a lack of resources or prioritization – typically bucketed as an IT function rather than a security one. Without proper visibility and threat detection, identity infrastructure provides ample opportunity for attackers to gain entry to critical systems. Identity has traditionally been managed by an organization's IT teams. With identity being a top attack vector, it's critical to bring together identity teams and the Security Operations Center (SOC) with ITDR so everyone is on the same page.



Without proper visibility and threat detection, identity infrastructure provides ample opportunity for attackers to gain entry to critical systems



The Talos Perspective

Cyber attackers are agile and often backed by substantial resources, including state sponsorship. This has led to an increase in advanced persistent threats which can target identities to gain access to sensitive information.

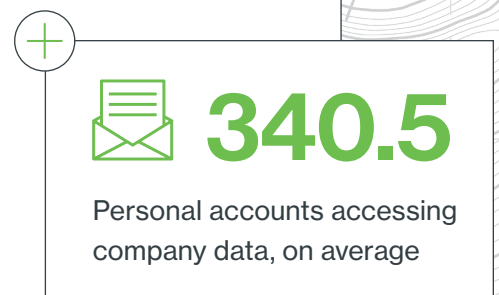
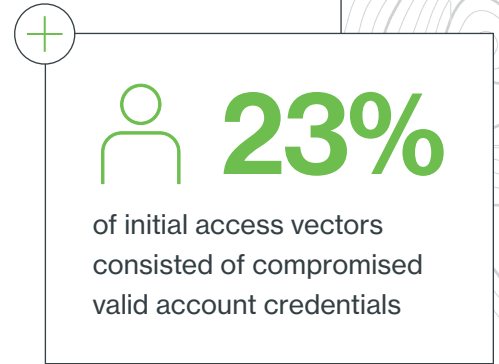
But this is nothing new. Attackers have targeted identities in their campaigns for many years. For example, on-premises identity directories or VPNs that lack additional protections have fallen victim to several attacks. Managing an increased range of identities is also an indicator of expanded attack surface. Talos Incident Response (Talos IR) has repeatedly seen attackers targeting vendor and contractor accounts (VCAs), which typically have expanded privileges and access. VCAs are often overlooked during account audits due to trust placed in the third party, making them an easy target for attackers.

The Talos 2023 Year in Review report saw compromised credentials on valid accounts making up 23% of initial access vectors, with use of valid accounts as the second-most common MITRE ATT&CK technique observed⁷. While one major vulnerability is improperly implemented MFA or lack thereof, in some engagements attackers were able to bypass MFA through MFA fatigue or push bombing attacks. ITDR can help surface the risks associated with valid account attacks and help correlate information from HRIS to identity providers and critical applications to help mitigate low-hanging fruit credential attacks.

Identity sprawl

Organizations are struggling with “identity sprawl,” which occurs when users have numerous accounts and identities managed by multiple systems that are not synchronized. This presents a continuous security risk and operational challenge for many security and IT teams.

Identity sprawl is a growing challenge. Talos IR research noted that it was challenging to identify how the credentials were compromised considering they were obtained from devices outside the company’s visibility, such as saved credentials on an employee’s personal device. One report shared that on average, companies have 340.5 personal accounts (Gmail, Yahoo, Hotmail, iCloud, etc.) with access to company data⁸. With the BYOD and perimeter-less work culture, a growing quantity of employee identities goes unchecked or unmanaged.



Footnotes:

7. From [Talos IR 2023 Year in Review](#), see “Telemetry Trends” pg. 6-7

8. From the [State of Identity Security](#) report (Oort), see Section 3 “Identity and Access Management: Poor Hygiene Enabling Attackers”

Establishing Device Trust



Gaining visibility into and securing myriad devices is still an ongoing battle, especially for organizations and industries that see a large diversity of endpoints such as higher education. Strong authentication mechanisms are at the heart of the security protocol – an essential line of defense in confirming the identities of users accessing the network. However, robust authentication is just one piece of the cybersecurity puzzle.

Ensuring users are using trusted devices and networks to access corporate data adds another layer of complexity. IT environments with complex supply chain operations, third-party partnerships, and contractor devices introduce risk of outside, unmanaged devices and unknown endpoints. This variability makes it challenging, if not impossible, to guarantee visibility and trust without a dedicated layer of security. Even with strong end-user authentication, the uncertainty of unmanaged network and device security remains a vulnerable chink in the armor.

In this context, identity-centric security is a dynamic and multifaceted endeavor. It demands a strategy that is comprehensive and adaptive, integrating advanced authentication, network security solutions, endpoint protection, continuous monitoring, and an informed and conscientious workforce.



A Diverse Device Environment

The starting point for establishing device trust is gaining a comprehensive understanding of the devices themselves – their operating systems, the browsers they use, their patch levels, and their compliance with corporate security policies. This understanding is critical because the security posture of any device is heavily influenced by the currency and integrity of its OS and browser. Outdated software can be riddled with unpatched vulnerabilities that are ripe for exploitation, turning an unassuming device into a Trojan horse within the network.

To determine if a device can be considered trustworthy, IT and security teams must be able to answer several key questions:

- Are there any unauthorized applications or software present?
- Is the device encrypted, and are its security settings configured according to the enterprise's standards?
- What OS is the device running?
- Is this OS still supported and receiving security updates?
- What browser versions are installed, and are they set to update automatically?

First, let's take a look at the browsers and OSes Duo customers use:

Mobile and non-traditional operating systems platforms show steady adoption, making up 61.8% of measured authentications. While we find that Windows is still the frontrunner, mixed IT environments can lead to more platform-agnostic security considerations.

Top OS		Mobile OS Usage	
Windows:	38.2%	iOS:	71.7%
iOS:	33.4%	Android:	28.2%
Mac OS X:	13.7%	Windows:	0.0%
Android:	13.1%		
Chrome OS:	1.1%		
Linux:	0.45%		

While Windows continues to lead the pack, we note that iOS is a strong second at 33.4% in the overall listings. Apple continues to rule the roost in the mobile category with the nearest contender being Android, which has a far lower adoption rate at 28.2%.





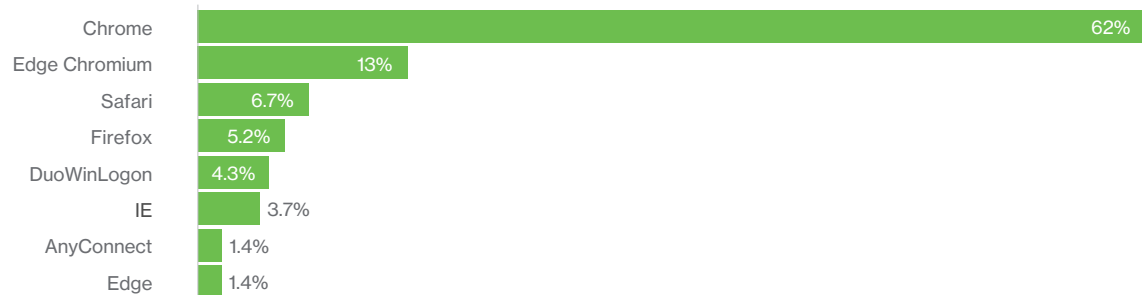
Chrome continues to dominate

Google Chrome continues to retain control as the top browser of record for businesses. No other browser even comes close to supplanting the leader.

Top Browsers

Chrome:	41.7%	Chrome Mobile:	7.7%	Firefox:	3.3%
Mobile Safari:	13%	Mobile Safari WebView:	4.7%	Chrome Mobile iOS:	2.9%
Edge Chromium:	12.6%	Safari:	4.6%	Edge:	0.1%

Percent of desktop authentications



Percent of mobile authentications

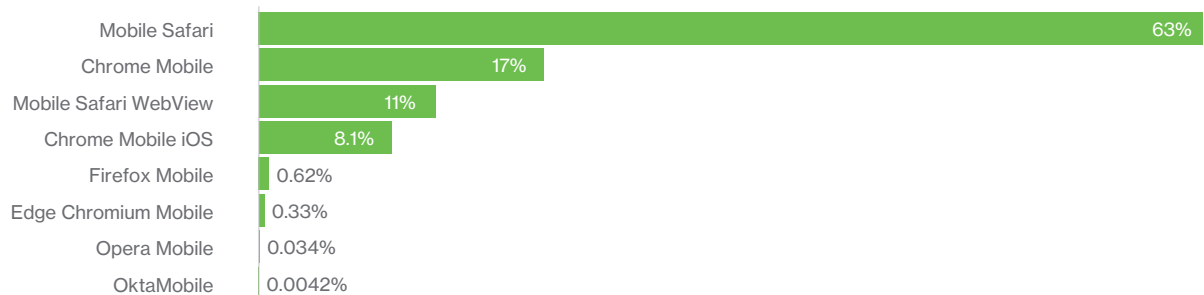


Figure 8 Different browsers used for authentication

Percent of Browsers

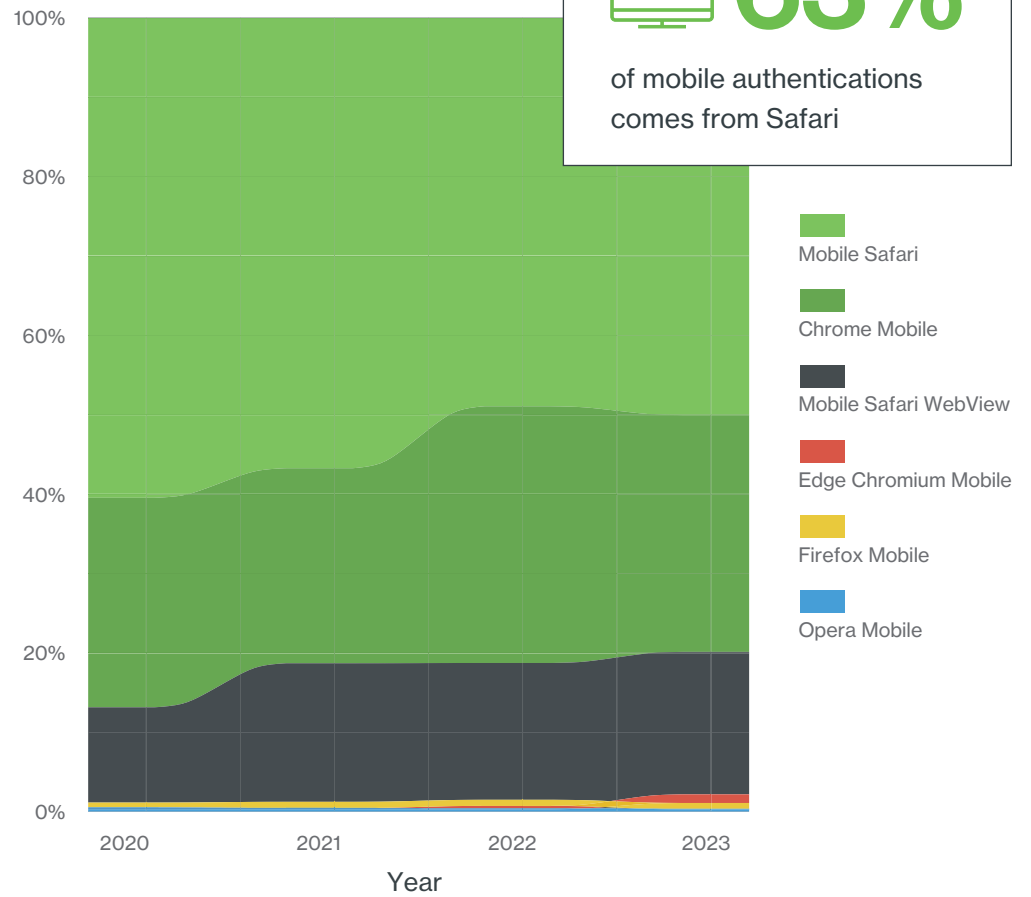


Figure 9 Percentage of mobile browsers used

IT environments that have a wider diversity of systems and browsers have a more pressing need to adopt more stringent device-based policies.



Device Visibility: Protecting What You Can't See

Maintaining device trust is a continuous process, requiring regular assessments and updates. This might involve automated compliance checks that verify whether a device is operating within the set parameters before granting access. Should a device fall short – say, running an OS version that's no longer supported – it can be flagged for review, blocked from accessing sensitive resources, or provided with limited, controlled access to mitigate potential risks.

This is important as applications and browsers like Google Chrome up the frequency of patches, accounting for performance and security bug fixes on a weekly basis. But how often are people relaunching and updating their applications? Of the 16 billion authentications measured, 62% of non-mobile authentications are attributed to the Chrome browser. The ability to see access device patch levels and prompt users to self-remediate out-of-date devices grows even more critical.

Visibility can be achieved through various tools and practices. Endpoint management systems, for instance, offer dashboards that provide real-time insights into the status of every device connected to the network. Automated inventory tools can keep track of the devices in use, their software versions, and their patch history. This monitoring is essential not just for ongoing management but also for responding to potential security incidents with speed and precision.



Authentication with Out-of-Date Software

Out-of-date failures

The percentage of failures due to out-of-date devices increased by 74.7% in 2023. This is despite the fact that the percentage of organizations with policies governing out-of-date devices decreased by 6.9%. The Asia-Pacific region ranked highest, with 3.8% of authentications occurring on an out-of-date browser.

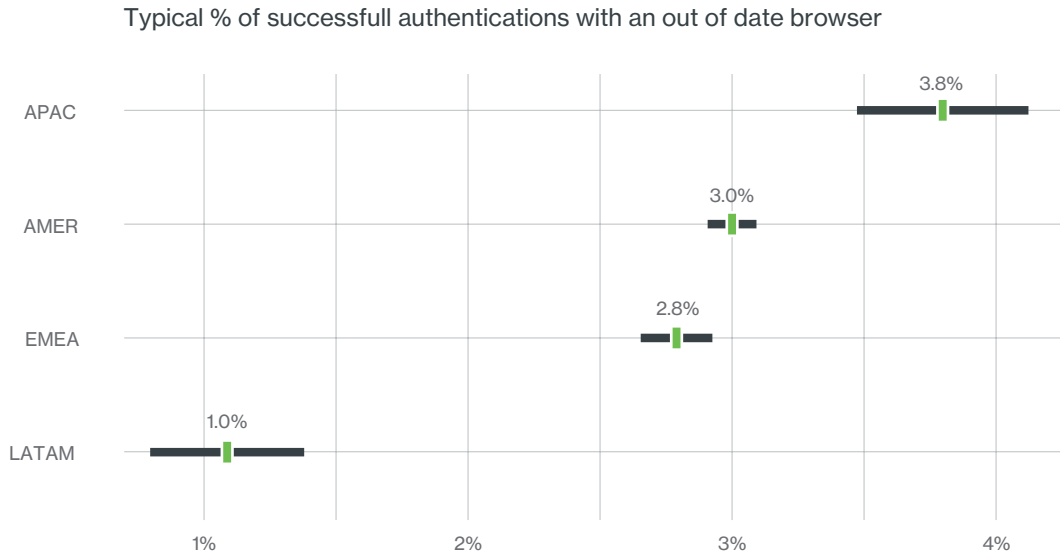


Figure 10 Typical (geometric mean) percentage of successful authentications using out-of-date browsers

The core of device trust lies in the ability to achieve complete visibility over the devices that are requesting access to corporate applications and data. In the ever-evolving geography of digital threats, authenticating within an IT environment that relies on outdated software is akin to navigating a ship with an old map.

Outdated software often contains unpatched vulnerabilities, which are like hidden, open backdoors for cyber attackers. These vulnerabilities are well-documented and easily exploitable as they stay in the public domain, providing a treasure map for malicious entities to gain unauthorized access. In this scenario, each authentication event is a gamble, increasing the chances that a security flaw can be used to compromise credentials.

Moreover, software that is past its support life no longer receives updates from its developers. This means that even as new threats emerge, the authentication mechanisms stay static and become increasingly ineffective against the sophisticated techniques employed by modern cyber adversaries. It is a static defense against a dynamic offense.

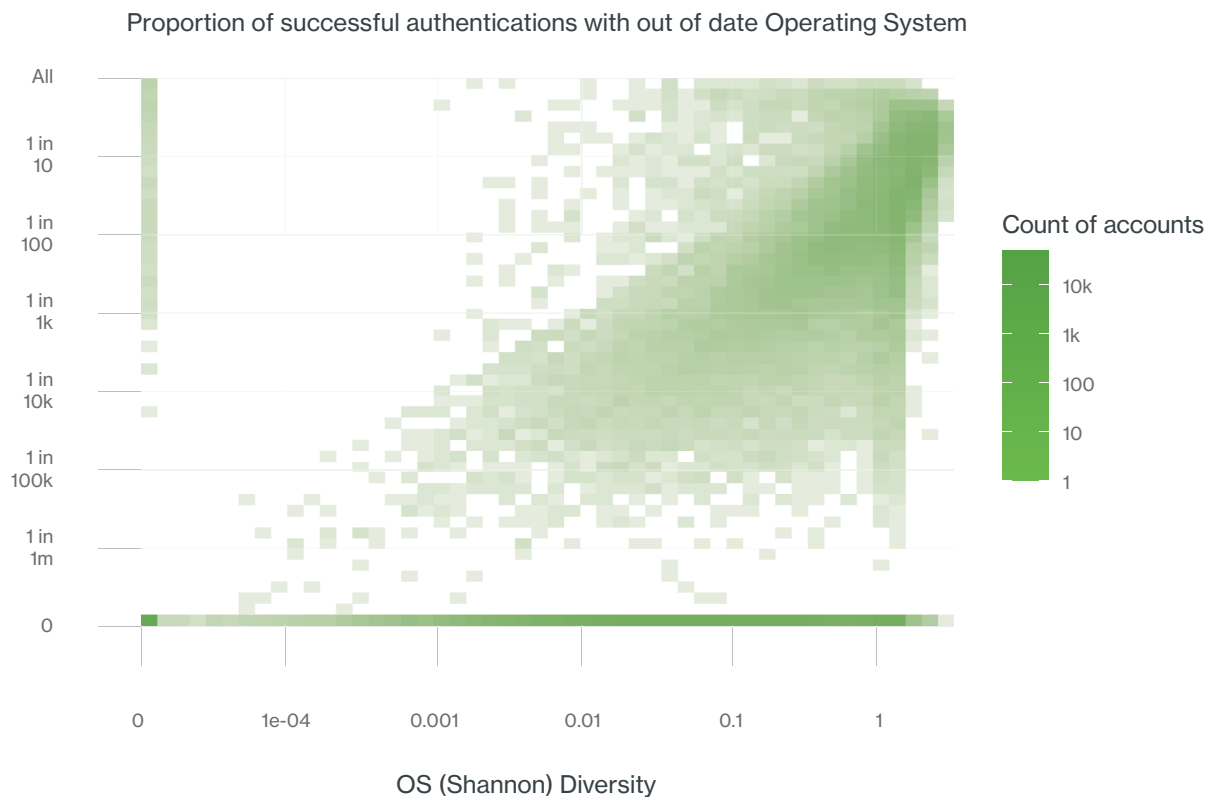


Figure 11 OS diversity and percentage of authentications that use an out-of-date operating system

The horizontal axis represents how “diverse” (in the ecological sense) a set of OSes is used to authenticate within an organization. A higher number means a wider variety of OSes that share an equal proportion of authentications. On the vertical axis is the proportion of authentications made with out-of-date OSes. The line across the bottom shows organizations that enforce OSes to be up to date, and the vertical line on the left shows organizations that use only a single OS.

Based on the data in Figure 11, the correlation shows that the more operating systems an organization allows to authenticate, the more likely it is those authentications will occur with an out-of-date OS. This becomes a fast reality for those expanding IT environments

To rely on outdated authentication software is to walk on a tightrope without a safety net. It’s an open invitation to security breaches, data theft, and the many consequences that follow. For an IT environment to remain secure and effective, it is imperative to invest in current, robust device trust methods that evolve in lockstep with the landscape of digital threats, providing visibility and enabling remediation. This is not just best practice; it is a fundamental tenet of responsible IT management in the digital age.



69%

Increase encryption usage

On Encryption & Firewall...

With the hybrid work model, organizations must also consider the use of virtual private networks (VPN), application of strict firewall policies, enforcement of data encryption, and secure setup of home networks. We looked at Duo Endpoint Health, particularly seeking to find out if organizations were generally increasing or decreasing their use of various protections. On an organization-by-organization basis, we see that, on average, organizations increased the percentage of encryption usage by 69%.

Device hygiene for the enterprise is an ongoing, evolving requirement, not a set-it-and-forget-it policy. This responsibility extends to the end-of-life process for devices, ensuring that all data is securely wiped and that devices are disposed of in a manner that does not pose a security threat. Similarly, user access levels must be adjusted to mitigate unnecessary or excessive privileges. Regular audits and compliance checks ensure that device and identity hygiene practices are not just in place but are effectively enforced and updated.

By diligently managing and monitoring operating system and browsers, among other device attributes, organizations can enforce a strong security posture and ensure that trust is not blindly given, but is based on verifiable, compliant device behavior.




Powerful Policy Controls

In a previous section, we highlighted the critical challenge of security debt – an accumulation of unaddressed risks and vulnerabilities that an organization must manage. Security debt can arise from various sources such as outdated software, legacy systems, technical shortcuts, and the delayed application of security patches. Reducing this debt is essential for maintaining a robust security posture and minimizing the organization’s exposure to potential breaches.

One of the most effective strategies for mitigating security debt is through the comprehensive management of risk. This includes identifying, assessing, and prioritizing the vulnerabilities within an organization’s IT infrastructure. By understanding where the greatest risks lie, an organization can allocate resources and efforts more effectively to address the most pressing security concerns first, thereby reducing the overall security debt.

Learning From When Authentications Fail

When reviewing the policy data, we uncovered some notable findings. In a move towards stronger methods of authentication, Duo Push-based authentication was present in 99.3% of all global policies. Mobile one-time passcodes were in 91.4% of policies defined. One of the more interesting findings was that WebAuthn was in 69.2% of the global policies.

 **69.2%**
of global policies included WebAuthn, a promising move towards stronger methods of authentication

It is just as important, if not more so, to measure the authentications that failed. It was noted that 5% of all measured authentications were ones that failed. When we further examined the data, we discovered that 28% of the failed authentications were due to the users not being enrolled in the system.

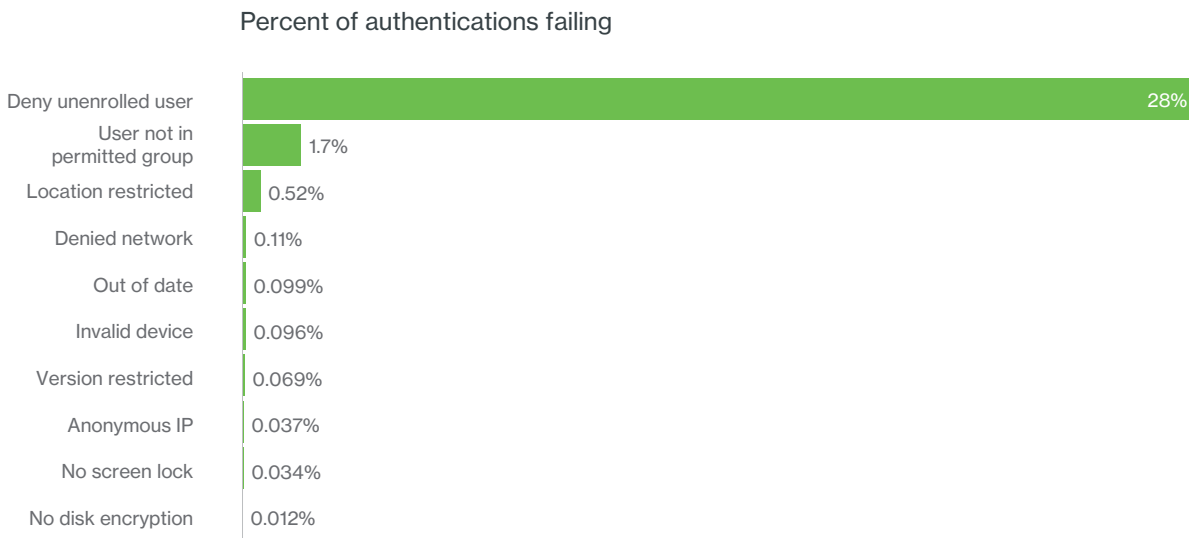


Figure 12 Percent of authentication failure reasons



Percent of accounts with policy

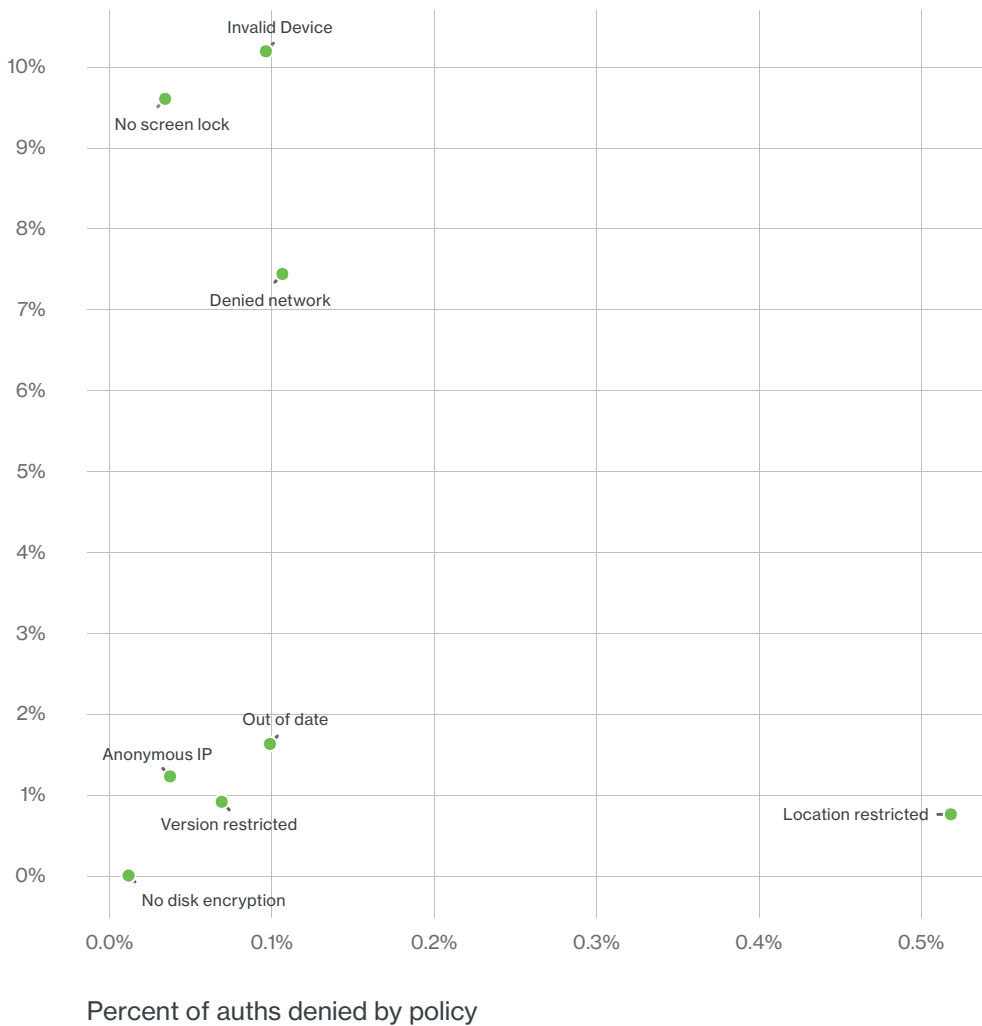


Figure 13 Percent of authentication failure reasons

Here we see that even though a little less than 1% of organizations have a policy concerning location, they account for a substantial proportion of failures. In removing failures caused by user enrollment, we can zoom in on those failed authentications influenceable by policy settings.

Benefits of Strong Device-Based Policies

A cornerstone of this risk reduction strategy is the implementation of uniform security policies across all assets in the environment. Device-based policies are especially critical because they provide a consistent security framework that applies to every device within the organization, irrespective of its location or user. These policies can control various aspects of device security, including the enforcement of strong authentication measures, the application of regular patches and updates, the configuration of firewalls and antivirus software, and the management of user privileges.

Uniform device-based policies are beneficial for several reasons:



Consistency: They ensure that every device adheres to the same security standards, which helps to cut weak links in the security chain that attackers might exploit.



Scalability: As the organization grows, new devices can be brought into the fold with established policies automatically applied, making it easier to manage security at scale.



Compliance: Device-based policies help organizations meet regulatory requirements by ensuring that all devices are compliant with industry standards and laws, reducing the risk of fines and other penalties.



Automation: These policies can often be enforced automatically, reducing the need for manual intervention and the associated human error.



Visibility and Control: Implementing uniform policies aids in the monitoring and control of device security, as deviations from the policy are easier to detect and remediate.

Top 3 Policy Groups to Reduce Security Debt

While reducing security debt is a complex, multifaceted endeavor, the foundation of this effort lies in the consistent application of comprehensive device-based policies. Such an approach addresses the security debt at its root, reducing risk and fostering a more secure, resilient organizational environment.

The interplay between access devices and security policies is a critical facet of an organization's cybersecurity framework. Rigorous security policies are set in place to ensure that devices attempting to access corporate resources meet certain standards of security before they are granted entry into the network. When a device does not meet these prescribed criteria, it triggers a series of automated responses aimed at safeguarding the organization's digital assets.

Duo's data shows that organizations that implement device-based policies most commonly block access from locations they consider unsecure and from where access should not originate. Organizations also tend to set policies to block invalid and out-of-date devices and those that don't feature a screen lock or disk encryption, as those simple security steps can protect the device and the data it transmits from being viewed by others.

Here are 3 types of policies that can help reduce complexity and increase security coverage:

01

Firstly, **geo-restrictions** are a common security measure, especially in scenarios involving sensitive data regulated by legal or corporate policies dictating data residency and sovereignty. When a user attempts to access the system from a location that is not whitelisted, the security protocol promptly intervenes, resulting in a failed authentication. This geographical gating is an effective deterrent against a range of threats, including unauthorized access by international cybercriminals.

Based off our research, many organizations do not take the necessary step to implement geography-based policies. In fact, we reported last year that the percentage of organizations who have any kind of policy denying specific geographic locations has dropped 20% since 2020. In 2023, 96.4% of organizations have no policy related to location (allow, deny, or require 2FA). However, among those enterprises that do deny geographic locations, they block either Russia or China 91% of the time and 63% of those organizations block both countries.



96.4%

of organizations have no policy related to location



Country denials over time

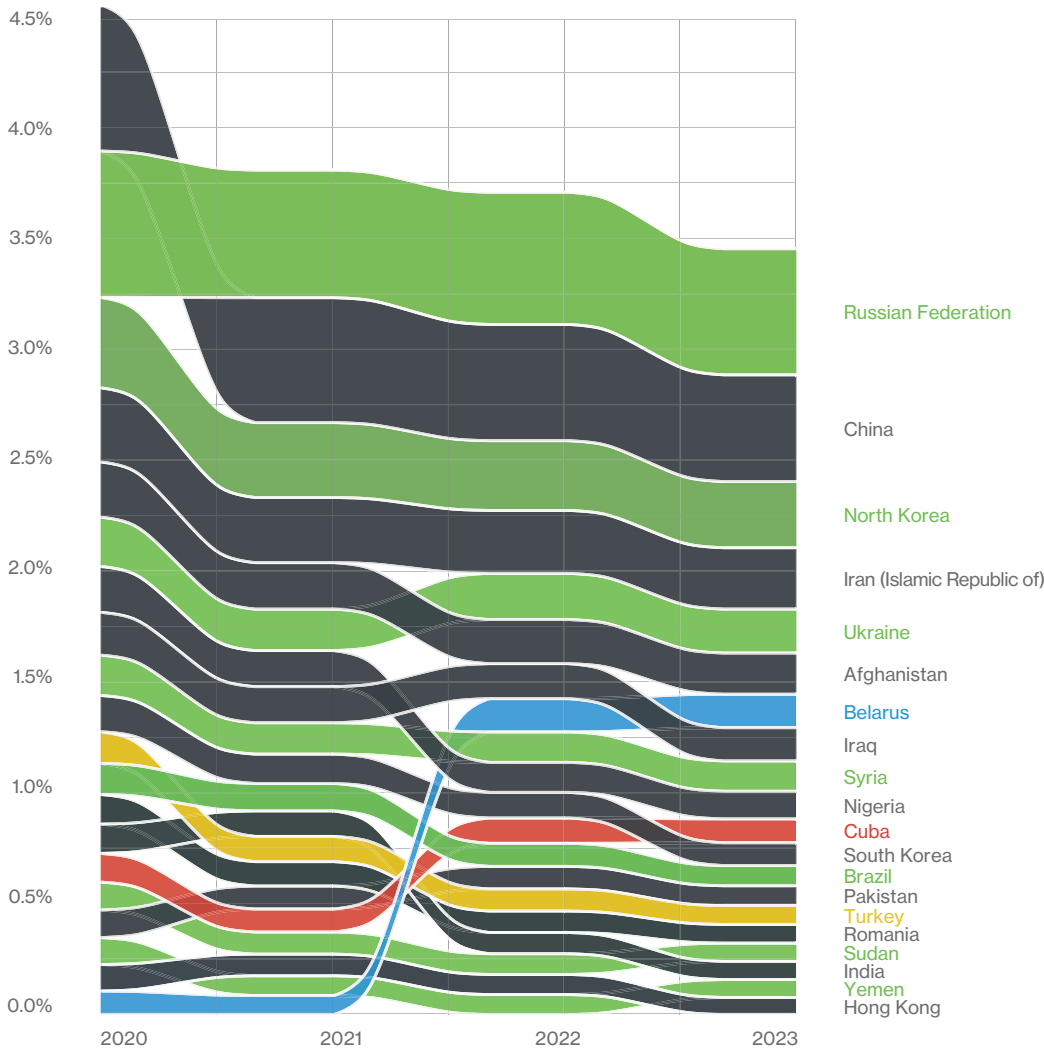


Figure 14 Percentage of accounts with denial policies focused on specific countries

02

Second, the use of **invalid or outdated devices** poses a significant risk. Devices that are no longer supported or have not been updated with the latest security patches are often riddled with vulnerabilities that can be exploited by cyber attackers. Security policies are designed to detect such devices based on their security posture – which includes the operating system version, installed security patches, and other critical security configurations. If a device is found wanting in any of these areas, the user may be barred from logging in or prompted to update their device to comply with the current security standards.

For example, mobile Safari is most likely to be used for successful authentications but also most likely to be out-of-date or end-of-life. In Figure 16, we report that most accounts only see 20-40% of browsers operating with the “latest” updates.

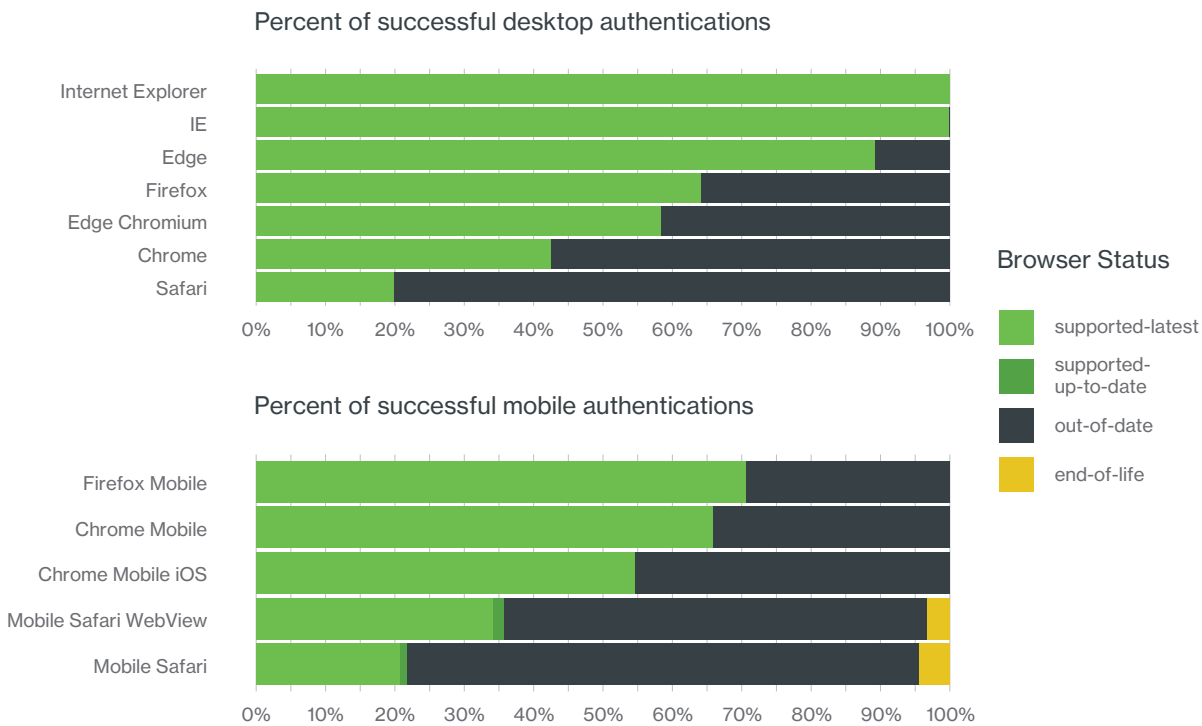


Figure 15 Percent of authentications by browser and browser update status

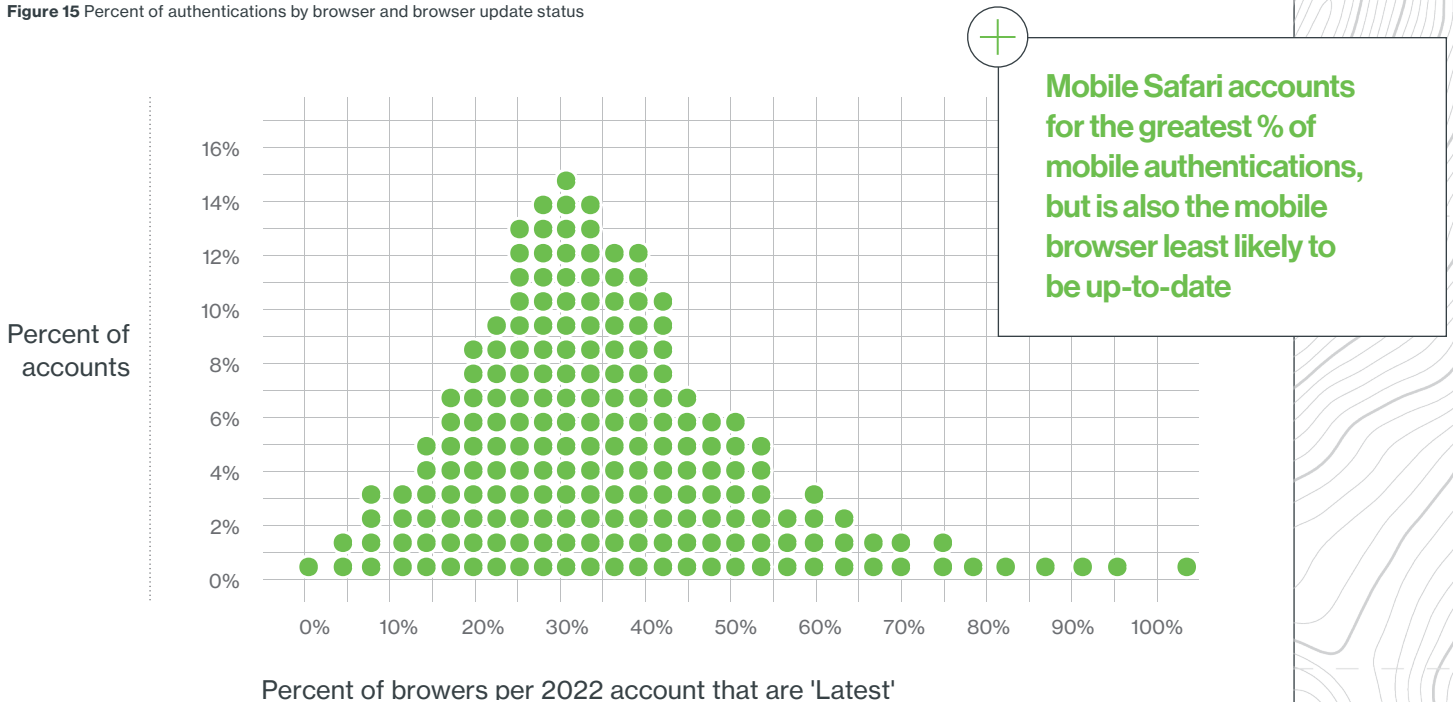


Figure 16 Percentage of up-to-date browsers within accounts



03

Third, granular access policies at the per-user group or per-application level lay the groundwork for **least privileged access**. Organizations today rely on their third-party ecosystems to supplement and support critical business functions. Aside from regulatory requirements, having unknown guest, dormant, or orphaned accounts can create additional management overhead and be a vector for unauthorized access to sensitive resources. Organizations should implement policies and procedures for managing accounts and limiting what they can access. This can include enforcing strong multi-factor authentication, regularly reviewing and auditing guest accounts, and disabling those that are no longer needed.



According to the State of Identity Security Report 2023, the average organization has many inactive accounts - more than 24% of its total identities. These accounts experience more than 500 attacks every month. To add to user base complexity, more than 3.24% of all identities are guest accounts.



The average organization sees over 500 attacks on inactive accounts each year

To ensure these policies are effective, organizations must also invest in employee education and awareness. After all, the most sophisticated policies can be undermined by human error. Organizations should educate their users about the potential risks associated with guest accounts and the importance of granting access only to trusted external users. Regular training sessions, simulations, and security drills can ingrain best practices and create a vigilant workforce capable of identifying and responding to security threats proactively.

Such stringent access controls, while occasionally inconvenient for users, are a necessary defense in an era where the sophistication of cyberattacks continues to escalate. They ensure that only compliant devices – and by extension, their users – can interact with the organization's systems, thus preserving the integrity, confidentiality, and availability of corporate data and services.



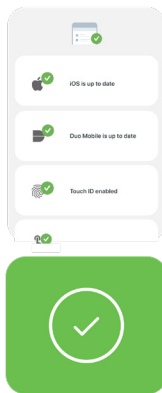
Closing Words



The future of identity security

Identity sprawl foments vulnerabilities. However, traditional identity infrastructure was built with IT operations in mind instead of security. Although the worlds of identity and security are coming together, in many larger organizations, security teams continue to work independently of IAM teams. Talent shortage makes securing the organization even more challenging. For small and mid-sized organizations, the IT department may just be a handful of people wearing lots of hats. A security team may not even exist yet. New security technologies such as identity threat detection and response can help bridge the gap between identity and security teams.

In addition to operational challenges, organizations battle with human capital constraints, namely the reliance on people to manage identities. Identity security is complex and requires an oversight of multiple elements, including:



User identity, which represents a specific user and is typically associated with unique credentials for authentication.



Device identity, which can be uniquely identified and associated with a user. The status and trustworthiness of a device can affect a user's ability to access certain resources.



Attributes or properties of an identity, such as a user's role, location, department, etc. Attributes can be used to determine and enforce access policies.



Permissions and access rights given to an identity, determining what resources that identity can access and what actions they can perform.



When IAM hygiene is poor, organizations' identity attack surfaces increase and provide additional opportunities to attackers. As more relationships are created between devices, attributes, identities and permissions, it becomes increasingly difficult to see and keep track of which identities are doing what.

Investigating incidents is also challenging without a solution that brings identity-related data together from multiple sources or helps pass contextualized posture information from IT to SOC. Visibility into misconfigured and unused accounts, including employees, contractors, and service accounts is also vital.

Having identity threat detection and response capabilities under one roof with access management is becoming a necessity. In tandem, these capabilities can help minimize chances of successful identity-based attacks while offering holistic coverage across identities and applications.

To address identity-based attacks with greater efficacy, IAM analytics need to be an inherent part of such a solution. This way, IT administrators can quickly address any security gaps by migrating from weak authentication to strong, phishing-resistant, multi-factor passwordless deployments across a customer's entire enterprise stack.

Context is the new MFA

In a world where data is king, but context is key, strong access management does not just continue to strengthen corporate security – it reshapes it. It addresses the inherent weaknesses of password-dependent systems and establishes a more robust, dynamic defense against the ever-evolving threat landscape.

Detailed logging and alerting mechanisms are essential to make sense of the noise. An attempt to authenticate via MFA can trigger alerts if the second or third factor fails, offering real-time threat detection and allowing for immediate response. This can greatly reduce the “dwell time,” the interval between a breach and its detection, which is crucial in mitigating the damage inflicted by a security incident.

We know that when navigating uncharted complexities, the steps we need to take can be easy to understand but hard to implement. As cyber threats grow in complexity and subtlety, adopting IAM best practices stands as a necessary evolution of security protocols—integral to safeguarding the assets, reputation, and future of any modern organization.



Recommendations

- Organization-wide adoption of **strong MFA** and moving towards requiring only phishing-resistant MFA such as FIDO2 security keys for privileged accounts.
- Enable **Verified Duo Push** which disarms push harassment and push fatigue attacks and puts your organization on the path towards **passwordless**.
- Ensure only **trusted devices**, managed or unmanaged, are granted access to corporate resources.
- Set data-informed user **authentication policies** that consider your organization's risk levels and focus points, with intelligent factor step-up that doesn't impede user productivity.
- Leverage a modern **single sign-on** solution as a policy enforcement tool to apply principles of zero trust and least privilege access for each application.
- Take advantage of solutions that assess user and device telemetry to identify known threat patterns and anomalies, like **Duo Risk-Based Authentication**. Evaluate login attempts for context and risk.
- Identify the IAM complexities in your environment with ITDR and assess weak points based on how much visibility you have. Leverage **Identity Threat Detection and Response** capabilities to get visibility across your identity ecosystem in a single, comprehensive interface.

Credits



Data Science

Cyentia Institute

Elizabeth Gilbert

Kevin Pelaez, PhD

Rose Putler, M.S.

Writers

Katherine Yang

Michael Parker

Slavka Bila

Production

Yolina Nenov

Taylor Stewart

Design & Dev

Amanda Cash

Chris Canote

Clayton Chu


Mary Jane Duty

Tony Ly



References

- [“2023 STATE OF IDENTITY SECURITY: Protecting the Workforce,”](#)
Oort, 2023
- [“Achieving Security Resilience: Findings from the Security Outcomes Report, Vol 3”](#)
Cisco, 10 January 2023
- [“Cisco Cybersecurity Readiness Index,”](#)
Cisco, March 2023
- [“Cisco Talos 2023 Year in Review,”](#)
Cisco Talos, 5 December 2023
- [“Incident Response Trends Q2 2023: Data Theft Extortion Rises, While Healthcare Is Still Most-Targeted Vertical,”](#)
Cisco Talos, 26 July 2023



Start your free 30-day trial and quickly protect all users, devices and applications at duo.com